AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Leah Bogdanowicz, having been duly sworn on oath, state as follows:

Affiant's Background

1. I have been employed as a Special Agent with the Federal Bureau of Investigation (FBI) since December of 2021. I am currently assigned to FBI's Albany Office, investigating cybercrimes including computer intrusions and fraud related crimes. I also have experience working counterintelligence matters. As a Special Agent with the FBI, I have received training related to cyber security and open-source intelligence. I have participated in the execution of search warrants involving physical and electronic evidence, including searches of email accounts and computers.

2. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested seizure warrant, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested seizure warrant.

3. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, and information I have obtained in the course of this investigation from witnesses having personal knowledge of the events and circumstances described herein and other law enforcement officers, all of whom I believe to be truthful and reliable.

Introduction

4. I submit this affidavit in support of an application for a warrant to seize all funds in the crytpocurrency wallet with address 0x095FeAE95aE837de18c45CD1c9c12845E080904B ("0x095") at Binance, the SUBJECT ACCOUNT.

5. Based on my training and experience and the facts as set forth in this affidavit, I submit that there exists probable cause to believe that funds within the SUBJECT ACCOUNT constitute proceeds of a "pig butchering[1]" fraud scheme or were involved in the commission of a fraudulent offense, in violation of Title 18, United States Code, Sections 1956 (laundering of monetary instruments and conspiracy to commit money laundering) and 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and therefore are:

a. Subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) and 19 U.S.C. §§ 1607-09 by 18 U.S.C. § 981(d); and

b. Subject to seizure via a civil seizure warrant under 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

6. This affidavit requests that the Court issue a warrant allowing law enforcement to seize the funds in the SUBJECT ACCOUNT and transfer them to a wallet controlled by law enforcement.

[1] According to chainalysis.com, "Romance scams, also known as 'pig butchering scams' for the way bad actors say they 'fatten up' their victims to extract the most possible value, are a large and growing problem with a significant crypto nexus. Romance scammers start by building a relationship over time with the victim (usually of a romantic nature, as the name implies), often initiating contact by pretending to have text messaged a wrong number or via dating apps. As the relationship deepens, the scammer will eventually push the victim to invest money (sometimes cryptocurrency, sometimes fiat) in a fake investment opportunity, and continue to do so until they eventually sever contact."

BACKGROUND

7. Based on my training, research, education, and experience, as well as conversations with other investigators with specifically related training and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency[2] or other cryptocurrencies. Examples of cryptocurrency are Bitcoin ("BTC"), Litecoin ("LTC"), Ethereum ("ETH"), Tether ("USDT"), dYdX ("DYDXUSDT"), Vulcan Forged ("PYR"), Graph ("GRT"), ImmutableX ("IMX"), Arweave ("ARUSDT"), PancakeSwap ("CAKE"), Bancor ("BNTUSDT"), and Cosmos ("ATOM"). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange (i.e. Kraken), or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger,

[2] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

run by the decentralized network, containing an immutable and historical record of every transaction[3]. Cryptocurrency is not illegal in the United States.

b. Bitcoin ("BTC") is the first decentralized cryptocurrency, created in 2009 to facilitate instant payments without central oversight. It uses peer-to-peer technology and cryptography to record transactions in a public ledger, called a blockchain, without central oversight.

c. Tether ("USDT") is an alternative type of cryptocurrency or altcoin token. Payments or transfers of value made with Tether are recorded in the blockchain network, but unlike decentralized cryptocurrencies like Bitcoin, Tether has some anatomical features of centralization. One centralized feature is that Tether is a stablecoin or a fiat-collateralized token that is backed by fiat currencies, or currencies issued by governments like the dollar and euro. Tether is backed with a matching one-to-one fiat amount, making it much less volatile than its counterpart, Bitcoin. Due to Tether's stable nature, wallet holders typically hedge their cryptocurrency holdings into Tether to stabilize valuation fluctuations and mitigate inherent cryptocurrency market volatility. "TetherUS" (USDT), also referred to as "Tether," is a cryptocurrency purportedly backed by United States (US) dollars. Tether was originally designed for each coin always to be worth $1, and the company responsible for issuing Tether purportedly maintained $1 in reserves for each Tether issued. As of January 1, 2024, one Tether coin was worth approximately $1 USD.

d. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26-36 characters long. Each public address is controlled and/or accessed using a unique corresponding private key—the cryptographic equivalent of a password or PIN— needed to access the address. Only the holder of an address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

e. Although cryptocurrencies such as bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track the flow of victims' funds.

f. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange.

g. Binance is a cryptocurrency exchange that offers trading, listing, fundraising, de-listing, withdrawing cryptocurrencies, and initial coin offerings (ICOs). It's the world's largest centralized crypto exchange, with 169 million registered users in over 180 countries. Binance is known for

altcoin trading, which is the practice of buying and selling altcoins, or alternative coins, on a daily basis with the goal of short-term profit. Altcoins are cryptocurrencies introduced after Bitcoin in 2009, and there are now over 5,000 of them. Many altcoins are similar to Bitcoin but have different features like distribution methods or mining algorithms. Some well-known altcoins include Ethereum, Ripple, Tether, Bitcoin Cash, Bitcoin SV, and Litecoin.

Facts Supporting Findings of Probable Cause

8. Since August 2023, the FBI has been investigating a fraud scheme being used to steal currency and cryptocurrency from individuals located throughout the United States. The scheme utilizes social engineering to lure victims into cryptocurrency investment via either directly messaging the victim though a messaging platform to discuss such investments or as a "wrong number" message that ends up leading into an investment discussion. Through discussions, the "threat actors", or Target Subjects, purporting to be investment experts convince these victims to exchange US dollars into cryptocurrency on a legitimate cryptocurrency exchange (i.e. Kraken, Gemini) and then instruct the victims to navigate to a specific website (i.e. www.safepal6.com), where the victims have a view of a fraudulent investment platform on their electronic devices. The fraudulent investment platforms appear to be legitimate cryptocurrency exchanges where the victims can log in and see their investments grow. However, as soon as the victims send their cryptocurrency, the funds begin making their way through a complex laundering scheme. Since January 2023, victims of the scheme have been convinced to transfer custody of their cryptocurrency to the Target Subjects under the guise of customer deposits to these cryptocurrency exchanges. The victims later discovered they were unable to withdraw funds they deposited to

their accounts, and in some cases, they were extorted for more cryptocurrency when attempting to withdraw. This scheme is known as pig butchering.

The Subject Account

9. The initial victim, Victim 1, is a Vermont resident who lost approximately $746,000 US dollars to the scheme detailed in paragraph 8, between February and April 2023. Victim 1 provided their initial transactions from Kraken, a known cryptocurrency exchange. Each of the initial cryptocurrency purchases were in Tether (USDT) on the Ethereum (ERC-20) blockchain. Through blockchain analysis, the victim funds were traced in USDT by investigators to a custodial wallet address at Binance - 0x095FeAE95aE837de18c45CD1c9c12845E080904B ("0x095") or the SUBJECT ACCOUNT. Between February and May 2023, up to 128,727 USDT of Victim 1's funds were deposited to the SUBJECT ACCOUNT, which is equal to approximately $128,692.76 US dollars. Various withdrawals and peer to peer exchanges occurred between May 2023 and April 1, 2024, resulting in a balance of 1.05231174 USDT, or a value of approximately $1 US dollar.

10. Victim 1's funds were not the only funds transferred into the SUBJECT ACCOUNT. A review of transaction records showed the SUBJECT ACCOUNT received cryptocurrency from over forty sending wallets—an unusual pattern for a legitimate wallet.

11. The SUBJECT ACCOUNT belongs to Binance User Identification (UID) number 292009713, hereinafter "User 292009713". User 292009713 has traded with over sixty different cryptocurrencies since October 2021, some of which are still available in the user's account. As noted above, User 292009713 has received cryptocurrency trades from over forty wallet addresses in twelve blockchains in the same time frame. Based on my conversations with other

federal agents familiar with investigating cryptocurrency crimes, the usage of several different cryptocurrency types, multiple sender wallets, and many blockchains are trends that are indicative of digital money laundering due to the intentional obfuscation of funds. Further, records for the SUBJECT ACCOUNT show many same day deposits and withdrawals, as well as deposits from multiple wallets on the same day. Based on my training and experience and conversations with other agents working in cryptocurrency, these patterns are also consistent with the cryptocurrency crime known as pig butchering.

12. Although almost all the Tether, including the Tether transferred from Victim 1, has been moved out of the SUBJECT ACCOUNT as of 4/1/2024. However, the SUBJECT ACCOUNT still contains .616899577002565578415O BTC, which is equivalent to approximately $42,430.54 US dollars. Based on my training and experience, I believe all funds in the SUBJECT ACCOUNT are the proceeds of fraud and subject to forfeiture.

Conclusion

13. Based on the facts and circumstances set forth in this affidavit, my training and experience, and information conveyed to me based on the training and experience of other agents working on cryptocurrency frauds, I submit that there exists probable cause to believe that SUBJECT ACCOUNT contains funds that constitute proceeds of a "pig butchering" fraud scheme or were involved in the commission of a fraudulent offense, in violation of Title 18, United States Code, Sections 1956 (laundering of monetary instruments and conspiracy to commit money laundering) and 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and therefore are:

a. Subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) and 19 U.S.C. §§ 1607-09 by 18 U.S.C. § 981(d); and

b. Subject to seizure via a civil seizure warrant under 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1)

I request that the Court issue a warrant to allow law enforcement to seize all cryptocurrency in the SUBJECT ACCOUNT and to transfer it to a wallet for the listed type of cryptocurrency controlled by law enforcement as follows:

a. Ethereum (ETH) - 0xba0D6620E494bAc8e745d954a291e16669923393

b. Tron (TRX) - TXcW1tvg8HDSfEdFM5MT8Ea7aXTpWqAd5F

c. Bitcoin (BTC) - bc1qangwtqlq7yrjlec6edp22uzum942g47zulnev4

d. Cosmos (ATOM) - cosmos1x5v7yl7rfr2c009mqqjhr42d6m6tyj6l58gzqa

Dated at Burlington, Vermont on this 19 day of April 2024.

Leah Bogdanowicz
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on April 19, 2024

Honorable Kevin J. Doyle
UNITED STATES MAGISTRATE JUDGE